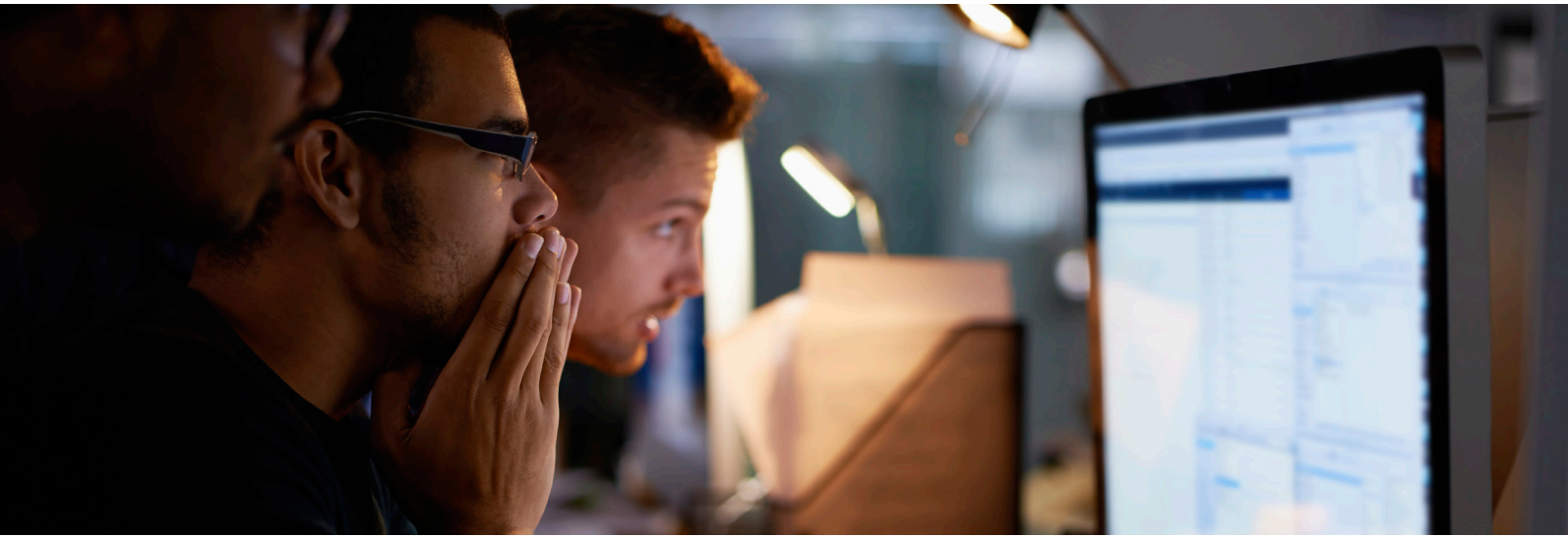
PROFESSIONAL SERVICES

Firewall Migration Methodology

Juniper NetScreen



Introduction

The purpose of this document is to outline the methodology or ‘’Method of Procedure” used by the Professional Services team when delivering a migration service from a Juniper Netscreen Firewall to a FortiGate configuration. The phases included in this document would be applicable to any third-party firewall, however, the aim is to highlight specifics for a Juniper Netscreen migration to provide specific detail on our approach.

This document is designed for Customer’s Security Teams (Engineering, Implementation or Support) to facilitate the preparation of a firewall migration. It should be noted that this document it is not a Scope of Work, nor should it be used as a Network Implementation Plan which requires detailed actions and planning. The high level phases when planning any firewall migration are;

The high level phases when planning any firewall migration are;

- Assessment & Requirements Analysis
- Planning, Architecture & Conversion
- Migration & Implementation

Assumptions

This document cannot cover all deployment scenarios therefore a list of assumptions is outlined below.

Elements in scope

- Firewalls operating in firewall-only/NAT/Router mode.

Elements not in scope

- A re-design of the existing architecture
- Application Layer Gateway (SIP, GTP, etc) and related activities
- Introduction of new features and functionality
- Migration of UTM services
- VPN client migration
- FortiManager and FortiAnalyzer or any other network or system integration

It should be noted that the migration of IPSEC VPNs requires a thorough design review and requires the development of a migration plan (based on a “one shot” or “phased” migration), which takes into consideration all potential risks, for example, interoperability with third party products and resource capacity.

Architectural Considerations

Juniper Netscreen and FortiGate firewalls have several common design elements, but there are implementation differences. Both ScreenOS and FortiOS can be considered “Zone” based firewalls; they have a strict association of security policies to ingress network interfaces. The FortiOS implementation is more flexible as policy enforcement can be performed using a global policy without any significant loss of granularity. Network Address Translation (NAT) is also handled differently; with ScreenOS NAT is configured per interface and then referenced in the main body of the policy. With the exception of address pools, within FortiOS the NAT policies are created on a per-policy basis. It is therefore essential to understand these differences in order to optimize the rule set conversion and adapt it to the customer’s requirements.

ScreenOS firewalls can be deployed with a combination of Virtual Systems (VSYS) and Virtual Routers (VRs). These services can facilitate unusual deployment scenarios such as mixed Layer 2 and Layer 3 enforcement domains and divergent/duplicate address space routing. Most ScreenOS functions have a FortiOS equivalency, but significant analysis will be required before these designs can be successfully migrated to a production network.

Both ScreenOS and FortiOS support Route mode and Policy mode branch office VPNs. However, many ScreenOS deployments favour Policy-based VPNs which may require a more complex migration to the Route mode VPNs that are preferred in FortiOS deployments.

With the help of tools to facilitate a configuration conversion, Professional Services utilize a strict methodology and work closely with Security Administrators, at the customer, to help them decide upon the optimal approach to enable a successful migration.

Assessment & Requirements Analysis

The purpose of this phase is to define the project baseline and ensure a clear understanding of the requirements and objectives of the project.
The first step in the process is for the customer to provide the existing configuration as well as a checklist of configuration and design elements. The checklist is aimed to review in particular:

- Objects & Groups, Nested Groups
- Policies
- Routing
- Interfaces
- Monitoring and Logging

A thorough review of the existing configuration is best practice before commencing any firewall migration, firstly to ensure an in-depth understanding of the environment, but also to identify areas for improvement in the logic of the rule base.
A firewall migration is also an opportunity for the customer to optimize the existing configuration. After many years of service, the rule set of a firewall can often become over-complex, some common examples of reasons for this are;

- Administrators prefer to add a new rule rather than editing an existing one
- Rules and objects can become obsolete because a service was decommissioned but the corresponding rule remains in the database
- There is no comment associated to the rule to understand its purpose or validity
- Over time a firewall can be managed by different technicians who do not follow the same implementation guidelines

To perform an initial optimization of the existing configuration, it is possible to use a conversion tool, however, at this stage a manual review and verification from the customer's security experts is required. It should be noted that based on field experience these two actions of configuration clean up, and, initial optimization can significantly reduce:

- The time allocated to the conversion and configuration review phase
- The number of policies active on the new system
- The number of conversion errors uncovered during the implementation and monitoring phase

Once the initial phase has been completed the migration kick-off meeting can take place, the key objectives of which, are to:
- Define requirements, project objectives and timing
- Discuss the checklist of configuration and design elements
- Discuss the conceptual differences between a FortiGate and Check Point firewall
- Discuss the optimization of the existing configuration

At the end of this phase an agreement should be reached on the key elements of the migration:
- Project timelines
- High-level design concepts
- Optimization objectives

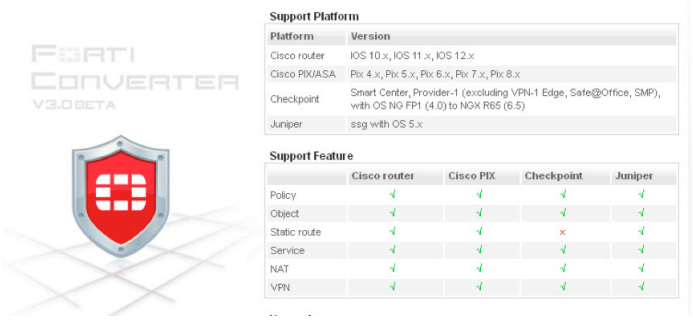
This ensures that when the configuration migration is complete, the new firewall rule set is documented and clearly understood by all parties.
A key action at this moment will be for the customer to implement a network freeze, whilst the target configuration is prepared and verified for deployment.

Planning, Architecture & Conversion

FortiConvertor

Fortinet has invested in the creation of a number of internal tools to facilitate the conversion of configuration files, in particular a tool called FortiConvertor. The purpose of this application is to assist in the conversion of configurations from third party firewalls.

FIGURE 1: FORTICONVERTOR



Rule Set Translation

Once the configuration has been processed by the FortiConvertor application it will still require manual verification. The amount of manual work required is dependent on the complexity of the rule set to be migrated. This process may be more onerous if the original rule set was not was not optimized, in particular with respect to the review of all Network Address Translation Rules and “Any” policies.

At this stage the active participation of the customer will be required, to provide additional explanations of individual rule sets. The consultant will also request “read-only” access to the firewall to be migrated at the customer site via the Web User Interface or Network Security manager (NSM) if available.

Configuration Pre-Staging

Once the rule set has been translated the consultant will load the configuration onto a test firewall in the FortiLabs to perform verification and testing. Once complete, details such as the routing tables are integrated. This will allow the full configuration to be prepared to a production standard before it is loaded onto the target firewall at the customer site.

The new firewall is therefore running the candidate configuration in order that the customer and Fortinet can access the device through the management network. This allows if required or feasible local testing of critical network applications.

Configuration Review

At this point in the project there is a full joint review of the proposed final configuration to ensure firstly, a final agreement, but also to provide a final opportunity for any additional clean-up of the rule base.

Product Knowledge Transfer

The Professional Services consultant will use the configuration review meeting to provide a Knowledge Transfer on the details of the configuration design, the logic and strategy of the rule sets and if required specifics of the hardware platforms utilized for the solution.

Migration & Implementation

This phase corresponds to the day when the migration will take place and the legacy Juniper Point firewall is decommissioned.

Pre-cutover Verifications

Prior to the service activation the customer is requested to run a series of tests to baseline the 'solution' before the migration. This step is achieved by:

- Writing scripts to test connectivity and service availability to critical resources. For example can end-stations can reach the internet, is mail is sent and received from designated mail servers.
- Writing test procedures to verify service availability.

Example test procedures:

- Can the mail server resolve against its DNS servers?
- Can a client send/receive emails?
- Are web servers able to reconnect to their database?
- Are the servers in the DMZ reachable from the Internet?

The customer is responsible for the creation of these procedures and scripts as they relate to their infrastructure and application base. It is also recommended that the security, server, and data networking teams take place in this activity to create a comprehensive snapshot of critical systems. Once the baseline is complete and recorded, it is possible to start the migration to the new solution.

Cutover

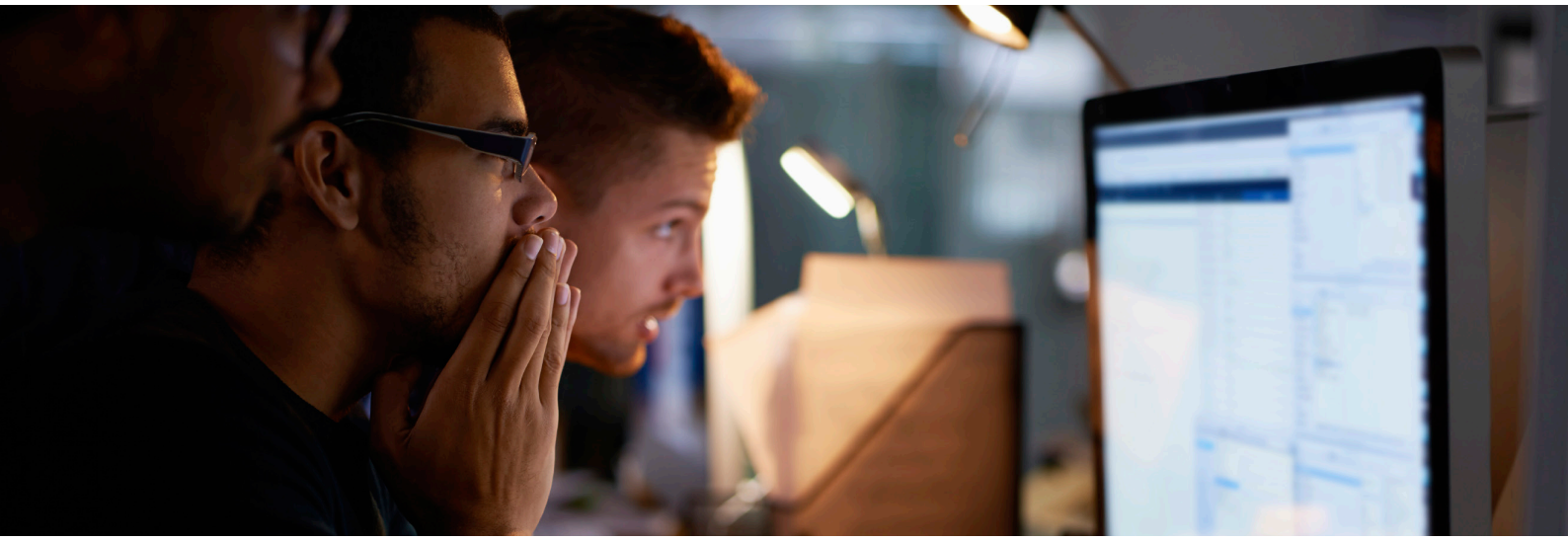
The legacy system is decommissioned and the FortiGate activated.
The Professional Services consultant performs a sanity check to ensure traffic is passed through the new firewall and that the system is behaving correctly. Once complete the customer is requested to perform a post-cutover validation.

Post-cutover Validation

The customer runs the baseline scripts and procedures, as performed during the "pre-cutover verification" phase. If required analysis is performed and configuration adjustments created in order to resolve any specific connectivity issues.

Acceptance

Once the validation phase is successful, the system remains in production. During a pre-agreed monitoring period (usually set to 15 calendar days), the customer may contact the Fortinet consultant to request assistance in resolving any connectivity issue directly related to the migration.



Migrating a complete Firewall infrastructure

If a customer has a requirement for a complete migration of their firewall infrastructure the first step would be to understand both the overall network design as well as any pre-defined project planning. With this information the consultant could start building a migration strategy with the customer to mitigate risk as well as ensure operational effectiveness for the project duration.

Although each customer environment is unique, in general the following approaches are typical for a large migration;

- Perform initial migrations in non-critical areas as a test exercise. This builds confidence in the solution as well as Fortinet skill sets within the customer as well as identifying any requirements for specific application handling. Some examples are firewalls deployed in non-critical areas such as general office deployments or a Disaster Recovery location.

- Parallel migrations whereby the legacy and FortiGate system is in operation for a period of time. This allows for full redundancy as well as allowing operational effectiveness to be built up over time.

- In the core of the network it may be feasible to migrate individual VDOMs or Virtual Firewalls individually to minimize the risk of ‘’one-shot” firewall migration.

- If the customer has very specific functionality the migration can be performed depending on the service requirement. This is typical in a telecommunications environment, where firewalls may be dedicated to functionality such as GTP.

www.fortinet.com

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480

Copyright © 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other resultsmay vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.